

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-233459

(43)Date of publication of application : 10.09.1993

(51)Int.Cl.

G06F 12/14

(21)Application number : 04-034936

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 21.02.1992

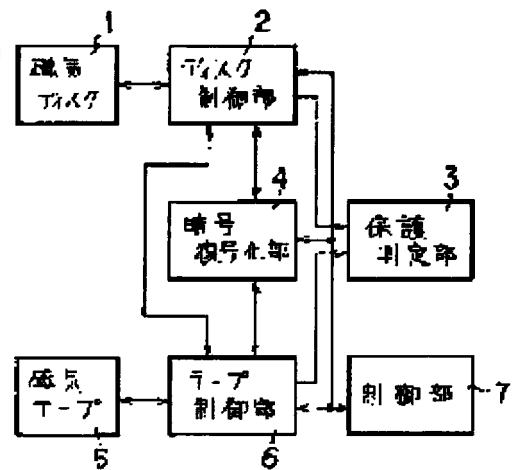
(72)Inventor : TOMOTA ICHIRO

(54) DATA BACKUP DEVICE

(57)Abstract:

PURPOSE: To encipher and back up data which should be secret.

CONSTITUTION: Data used by an information processing system for a specific process are stored on a magnetic disk 1 and a protection deciding means 3 decides whether or not all access principal bodies have the right for read access to the data read out of the magnetic disk 1 according to access right information added to the data. When it is decided that at least one of the access principal bodies does not have the right for read access are enciphered by an enciphering part 4 and recorded on a magnetic tape 5, and when it is decided that all of the access principal bodies have the right for read access, the data are recorded on the magnetic tape 5 as they are.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁(JP)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平5-233459

(43)公開日 平成5年(1993)9月10日

(51)Int.Cl.⁵

G 0 6 F 12/14

識別記号

3 2 0 B 9293-5B

片内整理番号

F I

技術表示箇所

審査請求 未請求 請求項の数2(全 7 頁)

(21)出願番号 特願平4-34936

(22)出願日 平成4年(1992)2月21日

(71)出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72)発明者 友田 一郎

神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝総合研究所内

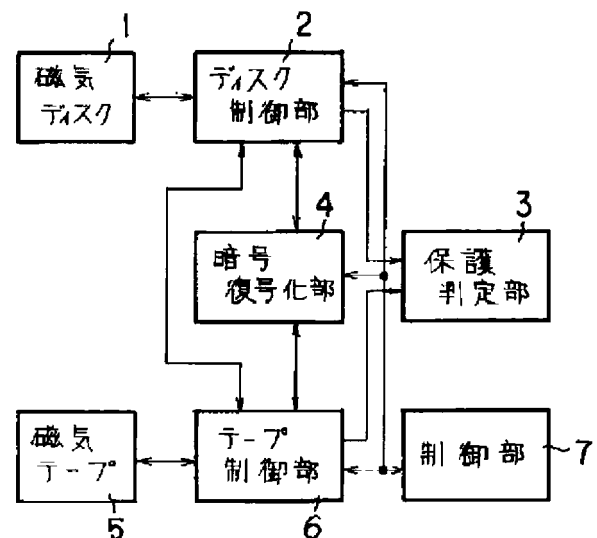
(74)代理人 弁理士 鈴江 武彦

(54)【発明の名称】 データバックアップ装置

(57)【要約】

【目的】本発明は、守秘の必要のあるデータについて暗号化してバックアップするようにしている。

【構成】情報処理システムでの所定の処理に用いられるデータを磁気ディスク1に記憶していて、この磁気ディスク1より読み出されたデータに対しあらかじめ付与されたアクセス権情報に基づいて全てのアクセス主体が前記データに対して読み出しアクセス権を持つか否かを保護判定部3で判定し、ここで少なくとも一つのアクセス主体が読み出しアクセス権を持っていないと判定されたデータについては暗号化部4で暗号化して磁気テープ5に記録し、一方、全てのアクセス主体に読み出しアクセス権を持っていると判定されたデータについては、このデータをそのまま磁気テープ5に記録するようにしている。



【特許請求の範囲】

【請求項1】 アクセス保護機能を備えた情報処理システムに用いられるデータバックアップ装置において、前記情報処理システムでの所定の処理に用いられるデータを記憶する第1の記憶媒体と、この第1の記憶媒体より読み出されたデータについてあらかじめ付与されたアクセス権情報に基づいてアクセス主体が前記データに対して読み出しアクセス権を持つか否かを判定する判定手段と、この判定手段により少なくとも一つのアクセス主体が読み出しアクセス権を持っていないと判定されたデータについて暗号化を実行する暗号化手段と、前記判定手段より全てのアクセス主体が読み出しアクセス権を持っていると判定されたデータについては該データをそのまま記録し前記少なくとも一つのアクセス主体が読み出しアクセス権を持っていないと判定されたデータについては前記暗号化手段で暗号化されたデータを記録する第2の記憶媒体を具備したことを特徴とするデータバックアップ装置。

【請求項2】 第2の記憶媒体は記録されるデータとともに該データにあらかじめ付与されたアクセス権情報を記録し、前記第2の記憶媒体より読み出されたデータに対し該データに付与されたアクセス権情報に基づいてアクセス主体が前記データに対して読み出しアクセス権を持つか否かを判定手段で判定し、該判定手段により少なくとも一つのアクセス主体が読み出しアクセス権を持っていないと判定されたデータについて復号化手段により復号化を実行し、前記判定手段より全てのアクセス主体が読み出しアクセス権を持っていると判定されたデータについては該データを、あるいは前記少なくとも一つのアクセス主体が読み出しアクセス権を持っていないと判定されたデータについては前記復号化手段で復号化されたデータをそれぞれ第1の記憶媒体に書込むことを特徴とする請求項1記載のデータバックアップ装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明はアクセス保護機能を備えた情報処理システムに用いられるデータバックアップ装置に関するものである。

【0002】

【従来の技術】 最近、各種の情報処理システムが用いられているが、このようなシステムでは、故障や操作ミスが原因でデータが破壊されることが多々ある。

【0003】 そこで、従来では、このような事態を想定して、システムで処理されるデータを複写して保存しておき、実際にデータが破壊された場合に、保存しておいたデータに基づいて元のデータを復元する、いわゆるバックアップを行うデータバックアップ装置が用いられている。

【0004】 一方、情報処理システムでは、一般にセキ

ュリティやプライバシーを保護する目的で、許さべからざるアクセスからデータを保護するものとして、アクセス保護機能が設けられている。

【0005】 この場合のアクセス保護機能は、アクセス権情報を設定するための手段とアクセス制御を行なう手段によって構成されている。ここで、アクセス権情報とは、システム内で処理するどのデータに対してどのアクセス主体がいかなるアクセスを行なう権利を持っているかについての情報で、アクセス主体とはアクセスを行なうもののことをいい、何を単位として個々のアクセス主体と考えるかはシステムにより異なり、例えばシステムに登録されている個々の利用者を個々のアクセス主体と考え、システム内で処理する個々のデータに対して個々の利用者がいかなるアクセスを行なう権利を持っているかという形でアクセス権情報を設定しアクセス保護を行なう場合が見受けられる。また、この他にも、システム中にある個々のコマンドを個々のアクセス主体と考えてアクセス保護を行なうものや、システムを構成する個々の処理装置を個々のアクセス主体と考えてハードウェア的にアクセス保護機能を実現するものも見受けられる。またアクセス制御手段は、アクセス主体によってデータに対しアクセスが行なわれようとした時に、前記アクセス権情報に基づいてそれが許可されるべきものか否かを判断し、許可されるべきでないアクセスを阻止することである。

【0006】

【発明が解決しようとする課題】 ところが、このようなアクセス保護機能を備えた情報処理システムにおいてデータのバックアップを行なう場合、以下のような問題点が発生していた。

【0007】 まず、情報処理システムにおいて処理過程にあるデータについては十分なアクセス保護をなし得ても、それをバックアップによって複写保存したものについては十分なアクセス保護を行なうのが困難なことが多く存在することである。例えば、磁気ディスク上のファイルシステムを磁気テープによりバックアップするような場合、一般にファイルシステムは磁気ディスク上のファイルに対してはアクセス保護を行うことができるが、磁気テープ上のファイルに対してまでアクセス保護を行うことができないことがある。

【0008】 このような場合、磁気ディスク上にあった時にはセキュリティ保護やプライバシー保護のために読み出す権利を持つ利用者を制限したファイルであっても、それをバックアップによって記録したものについては、本来読み出す権利のない利用者にも読み出し可能な状態になってしまうことが生じる。加えて、一般にバックアップを記録するための媒体は、例えば磁気テープなどのような取替可能な媒体が使われることが多く、しかもこれら媒体は持ち運びが容易であるために、盗まれる可能性もあった。

【0009】本発明は、上記事情に鑑みてなされたもので、バックアップによって保存されるデータに対してセキュリティ保護とプライバシー保護を安定して確保することができるデータバックアップ装置を提供することを目的とする。

【0010】

【課題を解決するための手段】本発明は、アクセス保護機能を備えた情報処理システムに用いられるデータバックアップ装置において、情報処理システムでの所定の処理に用いられるデータを記憶する第1の記憶媒体、この第1の記憶媒体より読み出されたデータについてあらかじめ付与されたアクセス権情報に基づいてアクセス主体が前記データに対して読み出しアクセス権を持つか否かを判定する判定手段、この判定手段により少なくとも一つのアクセス主体が読み出しアクセス権を持っていないと判定されたデータについて暗号化を実行する暗号化手段、判定手段より全てのアクセス主体が読み出しアクセス権を持っていると判定されたデータについては該データをそのまま記録し、少なくとも一つのアクセス主体が読み出しアクセス権を持っていないと判定されたデータについては前記暗号化手段で暗号化されたデータを記録する第2の記憶媒体により構成されている。

【0011】また、第2の記憶媒体は記録されるデータとともに該データにあらかじめ付与されたアクセス権情報を記録し、第2の記憶媒体より読み出されたデータに対し該データに付与されたアクセス権情報に基づいて全てのアクセス主体が前記データに対して読み出しアクセス権を持つか否かを判定手段で判定し、該判定手段により少なくとも一つのアクセス主体が読み出しアクセス権を持っていないと判定されたデータについて復号化手段により復号化を実行し、判定手段より全てのアクセス主体が読み出しアクセス権を持っていると判定されたデータについては該データをそのまま、あるいは前記少なくとも一つのアクセス主体が読み出しアクセス権を持っていないと判定されたデータについては前記復号化手段で復号化されたデータをそれぞれ第1の記憶媒体に書込むように構成されている。

【0012】

【作用】この結果、本発明によれば、少なくとも一つのアクセス主体が読出アクセス権を持っていないデータについては、守秘の必要のあるデータとして暗号化してバックアップし、全てのアクセス主体が読出アクセス権を持つデータについては、守秘の必要のないデータとして暗号化を行わずにそのままバックアップするようになり、バックアップデータについてのセキュリティ保護とプライバシー保護を確保することができる。

【0013】

【実施例】以下、本発明の一実施例を図面に従い説明する。

【0014】図1は同実施例のデータバックアップ装置

が適用されるオペレーティングシステムの概略構成を示している。図において、1は複数のファイルを格納可能にしたファイルシステムを構成する磁気ディスクで、この磁気ディスク1はディスク制御部2によりファイルの書き込み読み出しを制御されるようになっている。

【0015】ディスク制御部2には、保護判定部3を接続している。この保護判定部3は、後述するテープ制御部6にも接続していて、磁気ディスク1より読出されたファイル内容または後述する磁気テープ5より読出されたファイル内容について、これらファイルにあらかじめ設定されたアクセス権情報に基づいてすべてのアクセス主体が該ファイルに対して読出アクセス権を有するか否かを判定し、読み出しアクセス保護を行うものである。そして、この保護判定部3での判定結果に基づいて磁気ディスク1より読出されたファイル内容または後述する磁気テープ5より読出されたファイル内容を暗号・復号化部4または磁気テープ制御部5、ディスク制御部2に与えるようにしている。暗号・復号化部4は、周知のDES方式などを用いてファイルデータの暗号化または復号化するものである。

【0016】5は複数のバックアップ用ファイルを格納する磁気テープで、この磁気テープ5は、磁気テープ制御部6によりファイルの書き込み読み出しを制御されるようになっている。

【0017】7は制御部で、この制御部7は、ディスク制御部2、保護判定部3、暗号・復号化部4および磁気テープ制御部6の各制御を行うもので、これら各回路に対して制御指令を出力するものである。次に、以上のように構成した実施例の動作を説明する。

【0018】この場合、本実施例でバックアップを行う対象となるオペレーティングシステムのファイルシステムでは、磁気ディスク1に格納される個々のファイルについて、アクセス権情報としてU、G、Pの3つの属性が付与される。そして、このようなオペレーティングシステムは複数の利用者によって利用されるシステムで、利用者の集合として利用者グループを定義することができるようになっている。

【0019】ここで、各ファイルに付与される属性Uはファイルの所有権を持つ利用者の識別子を保持するものである。また、属性Gはそのファイルの所属する利用者グループの識別子を保持するものである。さらに、属性Pはそのファイルに対していかなる利用者がいかなるアクセス権を持つかを示す6ビットの2進整数値であり、その第0ビットはU属性に示す利用者がそのファイルを読み出す権利を持つか否かを、第1ビットはU属性に示す利用者がそのファイルに書き込む権利を持つか否かを、第2ビットはU属性に示す利用者ではないがG属性に示す利用者グループに所属する利用者がそのファイルを読み出す権利を持つか否かを、第3ビットはU属性に示す利用者ではないがG属性に示す利用者グループに所

属する利用者がそのファイルに書き込む権利を持つか否かを、第4ビットはU属性に示す利用者でもなくおかつG属性に示す利用者グループにも所属しない利用者がそのファイルを読み出す権利を持つか否かを、第5ビットはU属性に示す利用者でもなく、かつG属性に示す利用者グループにも所属しない利用者がそのファイルに書き込む権利を持つか否かを示している（いずれのビットもその値が1のとき権利を持つことを示し、0のとき持たないことを示す。）。

【0020】そして、このようなオペレーティングシステムにおけるバックアップ記録は、定期的にファイルシステムでの磁気ディスク1の稼働を停止し、その間に磁気ディスク1の中に存在する全てのファイルについて、その内容を磁気テープ6に複写することによって行なわれる。この場合、オペレーティングシステムによりバックアップの記録を行なうコマンドが提供される。この状態から、バックアップのためのデータ記録は、バックアップを指示するコマンドにより図2に示す処理フローに従って実行される。この場合、ディスク制御部2により、磁気ディスク1よりバックアップしようとするファイルを読み出す（ステップS21）。

【0021】次に、このようにして読み出したファイルを保護判定部3に与え、ファイルの属性値に基づき読出アクセス保護判定を行う（ステップS22）。この場合、ファイルの内容を読み出す権利が全ての利用者にあるか否かは、そのファイルのP属性の第0、第2、第4ビットが全て1であるか否かによって判定される。すなわちP属性の第0、第2、第4ビットをそれぞれ p_0 、 p_2 、 p_4 と表すと、読み出アクセス保護判定結果 c は $c = p_0 \wedge p_2 \wedge p_4$

により計算される。（ \wedge は論理積を意味する）

【0022】そして、ここでの判定結果として c の値が1の場合は、ファイルの暗号化は不必要と判断され（ステップS23）、ファイルは直接磁気テープ制御部6に与えられ、磁気テープ5に書込まれる（ステップS25）。

【0023】一方、保護判定部3の判定結果として c の値が0の場合には、ファイルの暗号化は必要と判断され（ステップS23）、ファイルは暗号・復号化部4に与えられる（ステップS24）。暗号・復号化部4では、暗号化が必要と判断されたファイルデータについて周知のDES方式などを用いて暗号化を行う。そして、この暗号化されたファイルの内容は、磁気テープ制御部6に与えられ磁気テープ5に書込まれるようになる（ステップS25）。この場合、ファイルに付与されたU属性、G属性、P属性のそれぞれの値もテープに書込まれるようになる。以下、同様にして磁気ディスク1に格納されたすべてのファイルについてバックアップ処理が行われる。

【0024】従って、このようにすれば少なくとも一つ

のアクセス主体が読出アクセス権を持っていないデータについては、守秘の必要のあるデータとして暗号化してバックアップし、全てのアクセス主体が読出アクセス権を持つデータについては、守秘の必要のないデータとして暗号化を行わずにそのままバックアップするようにできるので、バックアップによって保存されるデータに対して効率のよい守秘を得られ、バックアップデータに対するセキュリティやプライバシーが侵害される危険性を除去して、これらセキュリティ保護とプライバシー保護を安定して確保することができる。

【0025】次に、このようにして磁気テープ5に記録されたバックアップデータの復元は、バックアップの復元を指示するコマンドにより図3に示す処理フローに従って実行される。

【0026】この場合、磁気テープ制御部6により、磁気テープ5より復元しようとするファイルを読み出す（ステップS31）。この場合、上述したバックアップ記録の際に磁気テープ5に記録したU属性、G属性、P属性のそれぞれの値も読み出す。

【0027】次に、このようにして読み出したファイルを保護判定部3に与え、ファイルの属性値に基づき読出アクセス保護判定を行う（ステップS32）。この場合、磁気テープ5から復元されたP属性の値に基づいて、上述した記録の際に行なった読出アクセス保護判定と同様にして行なわれる。すなわち、磁気テープ5から復元されたP属性の第0、第2、第4ビットをそれぞれ p_0' 、 p_2' 、 p_4' と表すと、読出アクセス保護判定結果 c は

$$c = p_0' \wedge p_2' \wedge p_4'$$

により計算される。（ \wedge は論理積を意味する）

【0028】そして、ここでの判定結果として c の値が1の場合は、ファイルの復号化は不必要と判断され（ステップS33）、ファイルは直接ディスク制御部2に与えられ、磁気ディスク1に書込まれる（ステップS35）。

【0029】一方、保護判定部3の判定結果として c の値が0の場合には、ファイルの復号化は必要と判断され（ステップS33）、ファイルは暗号・復号化部4に与えられる（ステップS34）。暗号・復号化部4では、復号化が必要と判断されたファイルデータについて復号化を行う。そして、この復号化されたファイルの内容は、磁気ディスク制御部2に与えられ磁気ディスク1に書込まれるようになる（ステップS35）。以下、同様にして磁気テープ5にバックアップのため格納されたすべてのファイルが磁気ディスク1に復元されることになる。

【0030】従って、このようにしてもバックアップされたデータについて、少なくとも一つのアクセス主体が読出アクセス権を持っていないデータについては、守秘の必要のあるデータとして復号化して復元し、全てのア

クセス主体が読出アクセス権を持つデータについては、
 守秘の必要のないデータとして復号化することなく復元
 できるようになるので、バックアップによって保存され
 るデータの復元の際もデータに対して効率のよい守秘を
 得られ、復元されるデータに対するセキュリティやプ
 ライバシが侵害される危険性を除去して、これらセキ
 ュリティ保護とプライバシー保護を安定して確保する
 ことができる。本発明は、他の実施例として、電子メ
 ールシステムにおける通信内容のバックアップに適用
 することも可能である。

【0031】この場合、電子メールシステムにおけるメ
 ールには葉書形式と封書形式の2種類の形式があり、
 このうちの葉書形式のメールは比較的安価で提供され、
 内容はある定まった大きさ以内に制限され、内容の守
 秘は保証されていないが、封書形式のメールは比較
 的高価で提供され、内容の大きさは制限されず、内
 容の守秘が保証されている。

【0032】そこで、葉書型式のメールについては、そ
 のメールの送信者による読出アクセスと書込アクセス
 および全利用者による読出アクセスを許可し、また、
 封書型式のメールについては、そのメールの送信者
 による読出アクセスと書込アクセスおよびメールの
 受信者による読出アクセスのみを許可する。すなわ
 ち、メールの型式が葉書または封書のいずれかであ
 るかということをアクセス権情報とするようにして
 いる。

【0033】このメールシステムにおけるバックアップ
 は、2台のフロッピーディスク装置F0、F1を用い、
 利用者によりメールの送信要求があったときに葉書
 型式のメールはF0に、また封書型式のメールはF1
 にメールの内容を記録することにより実現している。

【0034】この場合、図4のフローチャートに示す
 ように、まず、読出アクセス保護判定を行う（ステ
 ップS41）。ここで、メールの内容が全ての利用者
 に読出可能であるか否かということは、そのメール
 が葉書型式であるか否かということと等価である
 ので、読出アクセス保護判定としては、バックア
 ュップ対象となっているメールの型式が何であ
 るかということを調べる。

【0035】そして、ここでの判定結果として葉書形
 式のメールと判定すると（ステップS42）、内容の
 暗号化を行わずにF0に記録する（ステップS43）。
 一方、ステップS42で封書形式のメールと判定す
 ると、メールの内容を暗号化して（ステップS44）、
 F1に記録するようになる（ステップS45）。

【0036】従って、電子メールシステムにおいても、
 上述したようにバックアップを行う場合と同様に
 して、バックアップによって保存されるメールに
 対して効率のよい守秘を得られ、バックアップメ
 ールに対するセキュリティやプライバシーが侵害
 される危険性を除去して、これらセキュリティ保
 護とプライバシー保護を安定して確保することが
 できる。なお、本発明は、上記実施例にのみ限
 定されず、要旨を変更しない範囲で適宜変形して
 実施できる。

【0037】

【発明の効果】本発明によれば、データのバックア
 ュップにおいて守秘の必要なデータについて、バ
 ックアップを通じてデータのセキュリティやプ
 ライバシの侵害の危険性を排除して、セキュリ
 ティ保護とプライバシー保護を安定して確保す
 ることができる。また、守秘の必要なデータ
 について暗号化、復号化を行うのみでバックア
 ュップを行うようにしているので、不必要な暗
 号化・復号化の計算を必要とすることなく、効
 率よくデータのバックアップを実現できる。

【図面の簡単な説明】

【図1】本発明の一実施例の概略構成を示す図。

【図2】図1の実施例の動作を説明するためのフ
 ローチャート。

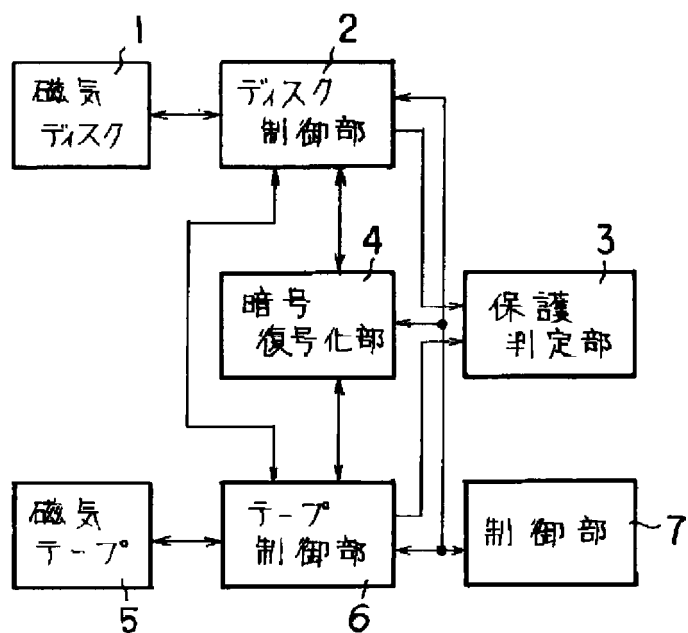
【図3】図1の実施例の動作を説明するためのフ
 ローチャート。

【図4】本発明の他の実施例を説明するためのフ
 ローチャート。

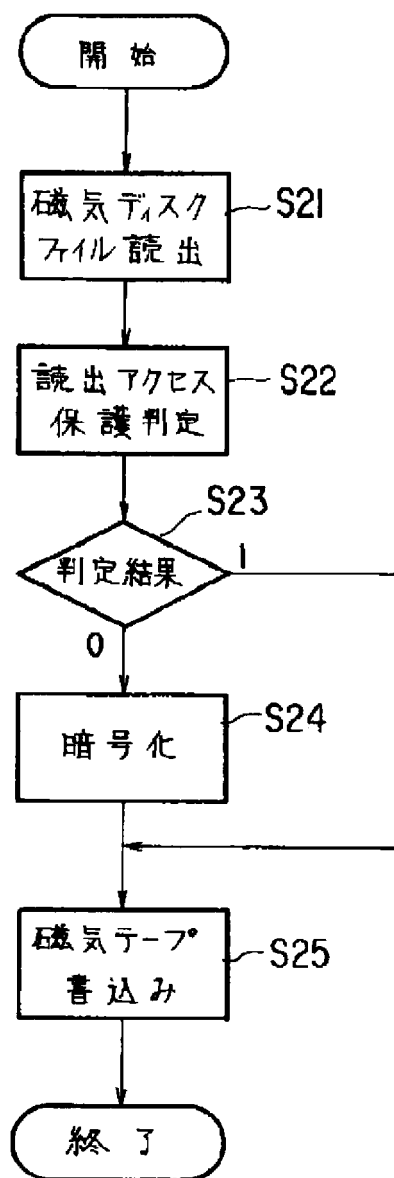
【符号の説明】

1…磁気ディスク、2…ディスク制御部、3…保
 護判定部、4…暗号・復号化部、5…磁気テー
 プ、6…テープ制御部、7…制御部。

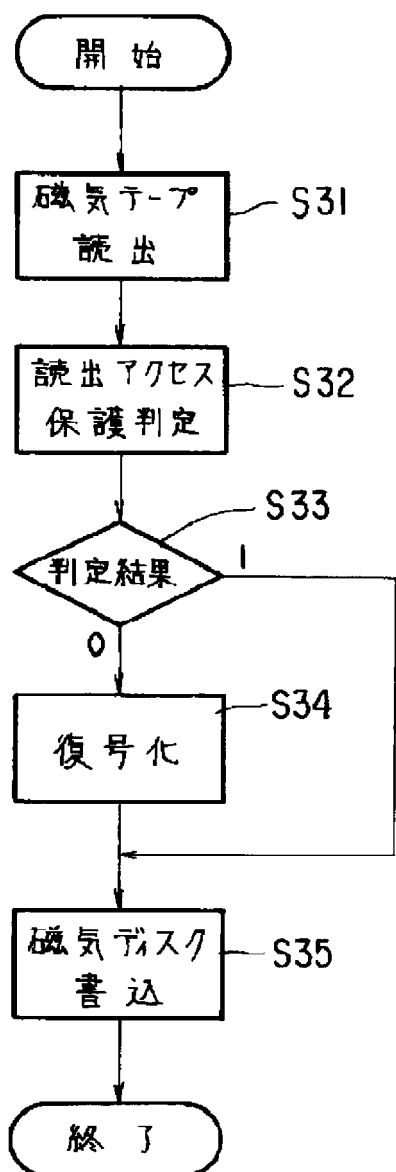
【図1】



【図2】



【図3】



【図4】

